UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/568,618	02/16/2006	Jovan Golic	09952.0025	9355

22852 7590 10/24/2008
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER
SHOLEMAN, ABU S

ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
10/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/568,618	**Applicant(s)** GOLIC, JOVAN	
	Examiner ABU SHOLEMAN	**Art Unit** 4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 February 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *42-82* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *42-82* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on *16 February 2006* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *02/16/2006*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This instant application having application NO. 10568618 filed on 02/16/2006 is presented for examination by the examiner.

Oath/Declaration

2. The applicant's oath/declaration had been reviewed by the examiner and is found to conform to the requirements prescribed in 37.C.F.R.1.63.

Information Disclosure Statement

3. The information discloser statement (IDS) submitted on 02/16/2006 has been acknowledged. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Drawings

4. The drawings were received on 02/16/2006. These drawings are acceptable for examination purposes.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 42 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. "selecting k out of 2^mk key bits" .

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 42-82 are rejected under 35 U.S.C.103(a) as being unpatentable over Viktor et al (Two Methods of Rijndael Implementation in Reconfigurable Hardware)(hereinafter Viktor) in view of Matsui et al (Patent Number: 5261003)(hereinafter Matsui).

As per claim 42, Viktor discloses "A combinatorial key-dependent network for encryption / decryption of input digital data of word size N into output digita data of the same word size " as (page 84, Fig 5, One round of the cipher is implemented as a mixture of combinatorial function of 128 bits of input plaintext and 128 bits of output cipher text), “comprising at least two layers” as (page 84, Fig 5, combinatorial function layer and round layer), “ each layer comprising at least an elementary building block” as (page 84, line 1-4, Internal data block is processed in 64 bit sub-blocks), “ each building block operating on an input block of bits having a word size n+m smaller than or equal to said word size N. for generating an output block of bits " as (page 84, Fig 5, combinatorial function block using input bits of 128 bits of plaintext that generates output of the cipher text of 128bits), but Viktor fails to disclose "a multiplexer circuit , receiving on a control input a first portion m of said block of bits, for selecting k out of 2 ^{m}K key bits on a k-bit output of said multiplexer circuit, said first portion of bits being transformed intact to an output of said building block ; and a transformation circuit, for transforming a remaining portion n of said input block of bits into transformed bits according to a reversible transformation chosen, by means of said selected k bits, among a plurality of reversible transformations implemented in said transformation circuit".

However, Matsui discloses “a multiplexer circuit , receiving on a control input a first portion m of said block of bits, for selecting k out of 2 ^{m}K key bits on a k-bit output of said multiplexer circuit, said first portion of bits being transformed intact to an output of said building block” as [(column 5-6 , line 47-48, line 25-29, Fig 1, Numerals 3 denotes 8 bytes of plaintext that divided into 4 more significant bits and 4 less significant bits, the selected key of the selector 25 generated from the less 4 less significant bit that goes to the processing block with 4 more significant bit); and " a transformation circuit, for transforming a remaining portion n of said input block of bits into transformed bits according to a reversible transformation chosen, by means of said selected k bits, among a plurality of reversible transformations implemented in said transformation circuit" as (column 5,line 62-67, Fig 1, numerals 33 designate an input step for inputting data to be scrambled , a selecting means or step for selecting one of a plurality of extended keys, a scramble processing means or step for processing the scrambling of the input data, and an output step for outputting the scrambled data).

Viktor and Matsui are analogous art because they are from the same field of endeavor of data block scrambling.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Viktor by including using divided text in the selector (inputting plaintext and key into the multiplexer) and the selector is generating a key that is scrambled with the remaining of the text and scrambling the text that taught by Matsui because it would provide a processing block by varying the extended cipher keys or the scramble functions depending on an input plaintext to improve random rate and security (column 3, line 58-65).

As per claim 43, Viktor discloses “wherein adjacent layers are connected by means of a fixed bit permutation block" as (page 78-79, section 2.1, line 11-17, byteRotation (permutation) connected to Multiplexer which is in the adjacent layer in the combinatorial circuit, Galois filed is fixed bit of data).

As per claim 44, Viktor discloses “comprising a plurality of fixed bit permutation blocks of the same type" as (page 84, line 1-2, Internal data block is processed in 64 bit or 32 bit sub-blocks in subsequent clock cycles, so permutation blocks are same type of data).

As per claim 45, Viktor discloses “comprising at least two different types of fixed bit permutation blocks" as (page 84, line 1-2, Internal data block is processed in 64 bit or 32 bit sub-blocks in subsequent clock cycles).

As per claim 46, Viktor discloses “ wherein bits in said first portion of said block of bits are used, in a next layer , as bits to be transformed" as (page 84, Fig1, a block of plaintext bits are coming into XORed from byteRotation, then it is XORed with Key to generated a transformed bits of Cipher text).

As per claim 47, Viktor discloses “wherein, for each building block, said first portion of said block of bits are extracted from at least two building blocks in a preceding layer, provided that m>=2" as (page 84, line 1-3, Embedded memory block sharing the data from internal block , the 128-bit cipher state, which is processed in 64(32) bit sub-blocks in 2^4 where is m that is the data portion , so m is m=4 in here, bit sub-blocks can be in 32(16) ,16(8) , 8(4) bit sub-blocks 2^2 where is m =2).

As per claim 48, Viktor discloses “ wherein , for each building block, said second portion of said block of bits are extracted from a least two building blocks in a preceding layer, provided that n>=2" as (page 84, line 1-3, Embedded memory block sharing the data from internal block , the 128-bit cipher state, which is processed in 64(32) bit sub-blocks in 2^4 where is n that is the data portion , so n is n=4 in here, bit sub-blocks can be in 32(16) ,16(8) , 8(4) bit sub-blocks 2^2 where is n =2).

As per claim 49, Viktor discloses “wherein each layer comprises at least two building blocks” as (page 79, Fig 1, There are two blocks in this cipher layer one is plaintext and other one is ciphertext).

As per claim 50, Viktor discloses “wherein said reversible transformations are such that each output bit of said transformed bits is a non-linear function of said first portion of said block of bits and of said k key bits, with the algebraic normal form containing at least one binary product involving both said first portion of said block of bits and said key bits" as (page 79, line 19-22, Inverse byte substitution is the non-linear step for reversible transformation).

As per claim 51, Viktor discloses “wherein said reversible transformation satisfy a criterion that the uncertainty of n input bits provided by uniformly random k key bits when the output n bits are known is equal to n bits" as (page 79, Fig 1, line 21-23, where is 128 bits = n bits coming into round key ki after invByteSubstitution and after round transformation the output is same as input).

As per claim 52, Viktor discloses “wherein said multiplexer circuit comprises as lookup table whose content is defined by the key” as (page 79 , line 18-21, In the table-lookup implementation, it is essential only non-linear step in the transformation round that has a round key).

As per claim 53, Viktor discloses " wherein said transformation circuit comprises XOR gates and controlled switches" as (page 84, Fig 5, the first step of this combinatorial circuit compose of XOR gates , there are plaintext and controlled switches come into XOR gates)

As per claim 54, Viktor discloses " wherein each XOR gate has two input bits and one output bit. one of the two input bits being a key bit, and each controlled switch has two input bits, two output bits and one control bit that determines if the input bits are swapped or not, said control bit being a key bit" as (page 84, Fig 5, XOR gate has two input. one is K key bits and other one is ByteRotation bits).

As per claim 55, Viktor discloses " wherein said multiplexer circuit has two control bits, four 3-bit inputs and one 3-bit output, and said transformation circuit comprises two XOR gates and one controlled switch" as (page 84, Fig 5, Multiplexer circuit has two controllers fist one is control key ki and 2nd one is MixColumn controlled key it could be any number of bit combination according to input bit).

As per claim 56, Viktor discloses “ wherein the three bits of said 3-bit output are connected respectively to a first input bit of each XOR gate and to the control bit of said controlled switch" as (page 84, Fig 5, Any number of cipher text output is connected to XORed input bit and contorlled key at round).

As per claim 57, Viktor discloses “ wherein a second input bit of each XOR gate is connected to a bit of said second portion of said block of bits” as (page 84, Fig 5, Input bit into XOR gate into is the part of input bit of ByteRotation block).

As per claim 58, Viktor discloses “ wherein the output bits of said XOR gates are connected to the two input bits of said controlled switch" as (page 84, Fig 5, Cipher text bit are connected to XOR gates that connected to any number of bits of ByteRotation).

As per claim 59, Viktor discloses “ wherein the two output bits of said controlled switch generate the transformed bits of said transformation circuit" as (page 84, Fig 5, Cipher text can be any number of output bits from the transformation circuit XOR).

As per claim 60, Viktor in view of Matsui discloses “the network according to claim 42", but fails to expressly disclose “comprising a plurality of building blocks of the same type".

However, Matsui discloses, disclose “comprising a plurality of building blocks of the same type" as (column 5, Fig 1, line 50-53, a plurality of processing blocks 9 has the same type of block).

As per claim 61, Matsui discloses “comprising at least two different types of building blocks” as (column 5, Fig 1, line 50-55, block 9 has two different types of blocks data , one is more significant bits and other is the extended keys block).

As per claim 62, Viktor discloses " wherein adjacent layers are connected by means of a block implementing a reversible liner function" as (page 79, Fig 1, InvMixColumn function is implemented as a reversible liner function).

As per claim 63, Viktor discloses “ wherein two additional input and output keys of word size N are bitwise XORed respectively with said input digital data and with said output digital data” as (page 84, Fig 1, K1 input and MaxColumn output of same input bits are XORed)

As per claim 64, Viktor discloses " wherein said key bits in each layer, having bit size k' , are generated from a smaller number of secret key bits, having bit size K, by means of a key expansion algorithm" as (page 80, Fig2, The key expansion algorithm uses bit-wise additions module bit values obtained from round addition).

As per claim 65, Viktor discloses “ wherein said k secret key bits are first expanded by means of liner transformation into k' key bits, using a linear code so that any subset of k'' expanded key bits are linearly independent , where k'' <=k " as (page 79, Fig1, MixColumn is a liner transformation of bits those bits are XORed with the key).

As per claim 66, Viktor discloses “ wherein said expanded key having bit size of k' is used as an input to a further combinatorial key-dependent network of block size $k^{‘}$ which is parameterized by a fixed randomly generated key satisfying the condition that every multiplexer implements balanced binary lookup tables” as (page 84, Fig 5, Multiplexer implements an expanded key in the combinatorial function from the lookup tables).

As per claim 67, Viktor discloses “ wherein the K'' bits produced after every two layers of said further combinatorial key-dependent network are used as said key bits from the multiplexer circuits within the layers of the combinatorial network" as (page 79, line , 5-7, Rounds key K are derived from the key schedule in the combinatorial function).

As per claim 68, Viktor discloses “ wherein said further combinatorial key-dependent network comprises a plurality of layers, each layer comprising a plurality of simplified building blocks" as (page 84, Fig 5, combinatorial function is the one building blocks), "a multiplexer having one input receiving one control bit which is passed to the output intact, for selecting one out of two key bits on a one bit output" as (page 84, Fig 5, 128 bits data inputting in Multiplexer and same outputting cipher text); and " a controlled switch having two input bits, two output bits and one control bit connected to the output of said multiplexer, said control bit determining if said two input bits are swapped or not" as (page 84, Fig 5, input bits and key bits are connected to Multiplexer output bit).

As per claim 81, Viktor discloses " A data processing device comprising a central processing unit , volatile or non-volatile memory, and at least a data, instruction or address bus" as (page 84, Fig 5, Cipher data processing unit of combinatorial bus or circuit), "comprising at least a combinatorial key-dependent network according to any one of claims 42 to 68" as (page 84, Fig 5, a combinatorial function) , "for encryption /decryption of digital data on said data, instruction , or address bus and /or into said memories" as (page 79, Fig 1, structure of encryption and decryption layer).

As per claim 82, Viktor discloses " A multimedia device for storing and playing copyright digital data comprising at least a combinatorial key-dependent network according to any one of claims 42 to 68" as (page 84, Fig 5, A combinatorial function that does data encryption for copyright), "for encryption /decryption of said copyright digital data" as (page 79, Fig 1, structure of encryption and decryption layer).

8. Claims 69-76 are rejected under 35 U.S.C.103(a) as being unpatentable over Viktor et al (Two Methods of Rijndael Implementation in Reconfigurable Hardware)(hereinafter Viktor) in view of Matsui et al (Patent Number: 5261003)(hereinafter Matsui).

As per claim 69, Viktor discloses “A block of secret-key-controlled cryptographic functions" as (page 84, Fig 5, A secret key controlled combinatorial functions), operating on an input block of bits for generating an output block of bits comprising" as (page 84, Fig 5, same input of plaintext and same out of the cipher text), but fails to expressly disclose "a multiplexer circuit , receiving on a control input a first portion m of said block of bits, for selecting k out of 2 ^{m}K key bits on a k-bit output of said multiplexer circuit, said first portion of bits being transformed intact to an output of said building block ; and a transformation circuit, for transforming a remaining portion n of said input block of bits into transformed bits according to a reversible transformation chosen, by means of said selected k bits, among a plurality of reversible transformations implemented in said transformation circuit".

However, Matsui discloses “a multiplexer circuit , receiving on a control input a first portion m of said block of bits, for selecting k out of 2 ^{m}K key bits on a k-bit output of said multiplexer circuit, said first portion of bits being transformed intact to an output of said building block” as (column 5-6 , Fig 1, Numerals 3 denotes 8 bytes of plaintext that divided into 4 more significant bits and 4 less significant bits, the selected key of the selector 25 generated from the less 4 less significant bit that goes to the processing block with 4 more significant bit); and " a transformation circuit, for transforming a remaining portion n of said input block of bits into transformed bits according to a reversible transformation chosen, by means of said selected k bits, among a plurality of reversible transformations implemented in said transformation circuit" as (column 5,line 62-67, Fig 1, numerals 33 designate an input step for inputting data to be scrambled , a selecting means or step for selecting one of a plurality of extended keys, a scramble processing means or step for processing the scrambling of the input data, and an output step for outputting the scrambled data).

Viktor and Matsui are analogous art because they are from the same field of endeavor of data block scrambling.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Viktor by including using divided text in the selector (inputting plaintext and key into the multiplexer) and the selector is generating a key that is scrambled with the remaining of the text and scrambling the text that taught by Matsui because it would provide a processing block by varying the extended cipher keys or the scramble functions depending on an input plaintext to improve random rate and security (column 3, line 58-65).

As per claim 70, Viktor discloses “Where in said transformation circuit comprises XOR gates and controlled switches" as (page 84, Fig 5, ByteRotation bits with key XORed in transformation circuit).

As per claim 71, Viktor discloses " wherein each XOR gate has two input bits and one output bit. one of the two input bits being a key bit, and each controlled switch has two input bits, two output bits and one control bit that determines if the input bits are swapped or not, said control bit being a key bit" as (page 84, Fig 5, XOR gate has two input. one is K key bits and other one is ByteRotation bits).

As per claim 72, Viktor discloses “ wherein said multiplexer circuit has two control bits, four 3-bit inputs and one 3-bit output, and said transformation circuit comprises two XOR gates and one controlled switch" as (page 84, Fig 5, Multiplexer circuit has two controllers fist one is control key ki and 2nd one is MixColumn controlled key it could be any number of bit combination according to input bit).

As per claim 73, Viktor discloses “ wherein the three bits of said 3-bit output are connected respectively to a first input bit of each XOR gate and to the control bit of said controlled switch" as (page 84, Fig 5, Any number of cipher text output is connected to XORed input bit and contorlled key at round).

As per claim 74, Viktor discloses " wherein a second input bit of each XOR gate is connected to a bit of said second portion of said block of bits" as (page 84, Fig 5, Input bit into XOR gate into is the part of input bit of ByteRotation block).

As per claim 75, Viktor discloses " wherein the output bits of said XOR gates are connected to the two input bits of said controlled switch" as (page 84, Fig 5, Cipher text bit are connected to XOR gates that connected to any number of bits of ByteRotation).

As per claim 76, Viktor discloses " wherein the two output bits of said controlled switch generate the transformed bits of said transformation circuit" as (page 84, Fig 5, Cipher text can be any number of output bits from the transformation circuit XOR).

9. Claims 77-80 are rejected under 35 U.S.C.103(a) as being unpatentable over Viktor et al (Two Methods of Rijndael Implementation in Reconfigurable Hardware)(hereinafter Viktor) in view of Matsui et al (Patent Number: 5261003)(hereinafter Matsui).

As per claim 77, Viktor discloses "A Method for encryption / decryption of input digital data of word size N into output digital data of the same word size " as (page 84, Fig 5, One round of the cipher is implemented as a mixture of combinatorial function of 128 bits of input data and 128 bits of output cipher data), but fails to expressly discloses " dividing said input digital data into blocks of bits, each having a word size n+m smaller than said word size N. each block of bits being divided into a first portion m and a second portion n; for each block of bits ; addressing a look up table containing 2^m k key bits, by means of said first portion m of bits , for selecting k out of 2^m k key bits, transferring intact said first portion m of bits to a first portion of transformed bits; selecting , by means of said selected k bits, a reversible transformation among a plurality of reversible transformations; applying said reversible transformation to said second portion n of bits, thus generating a second portion of transformed bits; collecting the transformed bits from each block into said output digital data.

However, Matsui discloses “ dividing said input digital data into blocks of bits, each having a word size n+m smaller than said word size N. each block of bits being divided into a first portion m and a second portion n; for each block of bits ; addressing a look up table containing 2^m k key bits, by means of said first portion m of bits , for selecting k out of 2^m k key bits, transferring intact said first portion m of bits to a first portion of transformed bits ” as (column 5-6 , Fig 1, Numerals 3 denotes 8 bytes of plaintext that divided into 4 more significant bits and 4 less significant bits, the selected key of the selector 25 generated from the less 4 less significant bit that goes to the processing block with 4 more significant bit); selecting , by means of said selected k bits, a reversible transformation among a plurality of reversible transformations; applying said reversible transformation to said second portion n of bits, thus generating a second portion of transformed bits; collecting the transformed bits from each block into said output digital data" as (column 5,line 62-67, Fig 1, numerals 33 designate an input step for inputting data to be scrambled , a selecting means or step for selecting one of a plurality of extended keys, a scramble processing means or step for processing the scrambling of the input data, and an output step for outputting the scrambled data).

Viktor and Matsui are analogous art because they are from the same field of endeavor of data block scrambling.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Viktor by including using divided text in the selector (inputting plaintext and key into the multiplexer) and the selector is generating a key that is scrambled with the remaining of the text and scrambling the text that taught by Matsui because it would provide a processing block by varying the extended cipher keys or the scramble functions depending on an input plaintext to improve random rate and security (column 3, line 58-65).

As per claim 78, Viktor discloses" where said step b) is reiterated on a block of bits comprising said first and second portions of previously transformed bits"as (page 84, Fig 5, After MixColumn, 128 bits is combining with previously transformed bits).

As per claim 79, Viktor discloses " wherein , before each reiteration of step b), a fixed bit permutation is applied to said previously transformed bits" as (page 78-79, section 2.1, line 11-17, byteRotation (permutation) connected to Multiplexer which is in the adjacent layer in the combinatorial circuit, Galois filed is fixed bit of data).

As per claim 80, Viktor discloses " wherein, before each reiteration of step b), a reversible linear function is applied to said previously transformed bits" as (page 81, Fig 4, InvMixColumn is linear transformation that is apply after cipher text transformation that is said previously transformed).

Conclusion

10. The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See MPEP 707.05(c).

11. The following reference teaches execution of trial data.

US 5261003

US 2002/0009196

US 6314187

US 5825888

US 2002/0166058

Two methods of Rijndael implementation of reconfigurable Hardware

12. Any inquiry concerning this communication or earlier communication form the examiner should be directed to Abu Sholeman whose telephone number is (571)270-7314. the examiner can normally be reached on Monday to Friday 8:30 AM to 5.00PM.

If attempts to reach the above noted Examiner by telephone are un successful, the Examiner's supervisor, Thomas Pham, can be reached at the following telephone number (571)2272-3689.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from the either Private PAIR or public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pari-direct.uspto.gov. Should your have questions on access to the Private PAIR system, contact the Electronic Business Center(EBC) at 866-217-9197(toll-free).

October 13, 2008
/A.S./

Abu Sholeman
Examiner
Art Unit 4148

/THOMAS K PHAM/
Supervisory Patent Examiner, Art Unit 4148